

# Automorphisms of Strongly Regular Graphs

S. De Winter, E. Kamischke, Z. Wang

November 14, 2014

## Abstract

In this article we generalize a theorem of Benson for generalized quadrangles to strongly regular graphs and directed strongly regular graphs. The main result provides numerical restrictions on the number of fixed vertices and the number of vertices mapped to adjacent vertices under an automorphism. It is explained how these results can be used when studying partial difference sets in Abelian groups and projective two-weight sets. The underlying ideas are linear algebraic in nature.

**Keywords**— Strongly regular graph; Benson’s theorem; partial difference set

**AMS classification**— 05C50, 05E30

## 1 Introduction

In 1970 Benson [1] provided a congruence that relates the parameters of a finite generalized quadrangle to the number of fixed points and the number of points mapped to collinear points under an automorphism. This result has turned out to be useful at various occasions in the theory of generalized quadrangles, see for example [12, 4]. In 2006 the first author [3] generalized this theorem to partial geometries and used it to obtain a characterization of the so-called Van Lint - Schrijver partial geometry. In 2010 Temmermans in her dissertation (see also [13]) provided further generalizations for other geometries, including partial quadrangles, and used these generalizations to study polarities of the geometries under investigation. Though interesting

results were obtained two observations stood out at this point that formed the starting point of this paper. On the one hand the Benson type results for generalized quadrangles and partial geometries were particularly elegant, whereas the result for partial quadrangles for example did not provide an elegant congruence, but rather a more complicated equation. This is due to the fact that a key matrix used in the proof has an eigenvalue equal to zero in the former cases, but not in the latter case. On the other hand, given the abundance of Benson type theorems for geometries whose collinearity graph is strongly regular one would expect the existence of a unifying theorem for strongly regular graphs. This paper will provide such unifying theorem while at the same time overcoming the problem that arose when the aforementioned matrix has no eigenvalue equal to zero. The aim of the article is not to provide a multitude of new applications, but rather to provide the theory, and point out some areas in which these results can be used through some basic examples.

## 2 Main Equalities and Congruences

### 2.1 Strongly regular graphs

We assume the reader to be familiar with strongly regular graphs. For more on these graphs see for example [6]. Let  $\mathcal{G}$  be a strongly regular graph  $\text{srg}(v, k, \lambda, \mu)$ , and let  $A$  be its adjacency matrix. Then the  $v \times v$ -matrix  $A$  has eigenvalues

$$\begin{aligned}\nu_1 &:= k, \\ \nu_2 &:= \frac{1}{2}(\lambda - \mu + \sqrt{\Delta}), \\ \nu_3 &:= \frac{1}{2}(\lambda - \mu - \sqrt{\Delta}),\end{aligned}$$

with respective multiplicities

$$\begin{aligned}m_1 &:= 1, \\ m_2 &:= \frac{1}{2} \left( v - 1 - \frac{2k + (v - 1)(\lambda - \mu)}{\sqrt{\Delta}} \right)\end{aligned}$$

and

$$m_3 := \frac{1}{2} \left( v - 1 + \frac{2k + (v - 1)(\lambda - \mu)}{\sqrt{\Delta}} \right),$$

where  $\Delta = (\lambda - \mu)^2 + 4(k - \mu) = (\nu_2 - \nu_3)^2$ . Furthermore these eigenvalues are integers if  $2k + (v - 1)(\lambda - \mu) \neq 0$ , that is, if  $\mathcal{G}$  is not a conference graph. In the case where  $\mathcal{G}$  is a conference graph, the eigenvalues are still integers provided  $v$  is a perfect square. We will call these eigenvalues and multiplicities also the eigenvalues and multiplicities of the strongly regular graph.

Let  $\phi$  be an automorphism of order  $n$  of the graph  $\mathcal{G}$ . Then  $\phi$  corresponds to a  $v \times v$ -permutation matrix  $P$  with the property that  $PAP^T = A$ . As  $P^{-1} = P^T$  we have  $PA = AP$ . Also  $P^n = I$ , where  $I$  is the  $v \times v$ -identity matrix. Let  $f_\phi$  denote the number of vertices fixed by  $\phi$ , and let  $g_\phi$  be the number of vertices mapped to adjacent vertices by  $\phi$  (this excludes fixed vertices). We will write  $f$  and  $g$  instead of  $f_\phi$  and  $g_\phi$  if the automorphism  $\phi$  is understood. Finally we will also need the following result. If  $P$  is a permutation matrix of order  $n$ , then the eigenvalues of  $P$  are the  $n$ th roots of unity, where the multiplicity of a given primitive  $d$ th root of unity equals  $\sum_{d|l} c_l$ , where  $c_l$  is the number of cycles of length  $l$  in the disjoint cycle decomposition of the permutation  $P$ .

**Theorem 2.1** *Let  $\mathcal{G}$  be a strongly regular graph  $\text{srg}(v, k, \lambda, \mu)$  whose adjacency matrix  $A$  has integer eigenvalues  $k, \nu_2$  and  $\nu_3$ . Let  $\phi$  be an automorphism of order  $n$  of  $\mathcal{G}$ , and let  $\mu(\cdot)$  be the Möbius function. Then for every integer  $r$  and all positive divisors  $d$  of  $n$ , there are non-negative integers  $a_d$  and  $b_d$  such that*

$$k - r + \sum_{d|n} a_d \mu(d)(\nu_2 - r) + \sum_{d|n} b_d \mu(d)(\nu_3 - r) = -rf + g, \quad (1)$$

where  $f$  is the number of fixed vertices of  $\phi$  and  $g$  is the number of vertices that are adjacent to their image under  $\phi$ . Furthermore  $a_1 + b_1 = c - 1$ , where  $c$  is the number of cycles in the disjoint cycle decomposition of  $\phi$ , and  $a_d + b_d = \sum_{d|l} c_l$ ,  $d \neq 1$ , where  $c_l$  is the number of cycles of length  $l$  of  $\phi$ . As a consequence the following congruence holds:

$$k - \nu_3 \equiv -\nu_3 f + g \pmod{\sqrt{\Delta}}. \quad (2)$$

**Proof.** Let  $M$  be the matrix  $M = A - rI$ . Then obviously  $M$  has integer eigenvalues  $\tau_1 = k - r$ ,  $\tau_2 = \nu_2 - r$  and  $\tau_3 = \nu_3 - r$ , with respective multiplicities  $m_1, m_2$  and  $m_3$ . If  $P$  is the permutation matrix corresponding to  $\phi$ , then clearly  $PM = MP$ , and hence

$(PM)^n = P^n M^n = M^n$ . It follows that the eigenvalues of  $PM$  are the eigenvalues of  $M$  multiplied with appropriate  $n$ th roots of unity. As the sum of the elements in each row of  $M$  equals  $k - r$ , the same will hold for  $PM$ , and hence  $k - r$  is an eigenvalue of  $PM$ . This eigenvalue clearly has multiplicity  $m_1 = 1$ . Now let  $d$  be a positive divisor of  $n$ , and let  $\xi_d$  be a primitive  $d$ th root of unity. As the eigenvalues of  $M$  are integers, it follows (see for example Lemma 3.1 of [13]) that the multiplicity (which might be zero) of the eigenvalue  $\xi_d(\nu_2 - r)$  of  $PM$  will only depend on  $d$ , and not on the specific primitive  $d$ th root of unity. Denote this multiplicity by  $a_d$ . Analogously the multiplicity (which might be zero) of the eigenvalue  $\xi_d(\nu_3 - r)$  of  $PM$  will only depend on  $d$ . Denote this multiplicity by  $b_d$ . Also, as the sum of all primitive  $d$ th roots of unity equals  $\mu(d)$ , where  $\mu$  is the Möbius function, we obtain

$$\text{trace}(PM) = k - r + \sum_{d|n} a_d \mu(d)(\nu_2 - r) + \sum_{d|n} b_d \mu(d)(\nu_3 - r).$$

On the other hand the trace of  $PM$  must equal  $-rf + g$ , and hence

$$k - r + \sum_{d|n} a_d \mu(d)(\nu_2 - r) + \sum_{d|n} b_d \mu(d)(\nu_3 - r) = -rf + g. \quad (3)$$

Setting  $r = \nu_3$  we obtain

$$k - \nu_3 + \sum_{d|n} a_d \mu(d)(\nu_2 - \nu_3) = -\nu_3 f + g \quad (4)$$

and

$$k - \nu_3 \equiv -\nu_3 f + g \pmod{\sqrt{\Delta}}. \quad (5)$$

Finally, in order to compute  $a_d + b_d$ , we note that as  $P$  and  $M$  commute and are diagonalizable they are simultaneously diagonalizable (see for example Theorem 1.3.12 in [7]). Let  $\mathcal{B}$  be a common eigenbasis for  $P$  and  $M$ , and let  $\mathcal{V}_d := \{v_1, v_2, \dots, v_m\} \subset \mathcal{B}$  be a basis for the eigenspace of  $P$  corresponding to the eigenvalue  $\xi_d$  of  $P$ . If  $d = 1$  we see that exactly one of the vectors in  $\mathcal{V}$  is an eigenvector for the eigenvalue  $k - r$  of  $M$ , exactly  $a_d$  of the vectors in  $\mathcal{V}$  are eigenvectors for the eigenvalue  $\nu_2 - r$  of  $M$ , and exactly  $b_d$  of the vectors in  $\mathcal{V}$  are eigenvectors for the eigenvalue  $\nu_3 - r$  of  $M$ . Hence  $1 + a_1 + b_1 = c$ , where  $c$  is the number of cycles in the disjoint cycle decomposition of  $\phi$ . Now let  $d \neq 1$ . Then exactly  $a_d$  of the vectors in  $\mathcal{V}$  are eigenvectors for the eigenvalue

$\nu_2 - r$  of  $M$ , and exactly  $b_d$  of the vectors in  $\mathcal{V}$  are eigenvectors for the eigenvalue  $\nu_3 - r$  of  $M$ . Hence  $a_d + b_d = \sum_{d|l} c_l$ , where  $c_l$  is the number of cycles of length  $l$  in the disjoint cycle decomposition of  $\phi$ . This proves the theorem.  $\square$

This theorem generalizes the previously known Benson type theorems for generalized quadrangles, partial geometries, and partial quadrangles. The key difference with those previous results is that our proof relies on the matrix  $M$ , which simply is the adjacency matrix plus an arbitrary integer multiple of the identity, rather than relying on the matrix  $NN^T$ , where  $N$  is the incidence matrix of the studied geometry. This matrix  $NN^T$  always equals  $A + (t + 1)I$ , where  $A$  is the adjacency matrix of the point graph of the geometry, and  $t + 1$  is the number of lines through a point in the geometry. But  $-t - 1$  is not necessarily an eigenvalue of  $A$  (for example in the case of partial quadrangles), and hence one cannot guarantee that  $NN^T$  has an eigenvalue equal to zero. However, it is exactly the fact that  $M$  can be made to have an eigenvalue equal to zero that allows us to deduce Equation (4) and Congruence (5) in general. Also the restriction on the value of  $a_d + b_d$  is new. Though Congruence (5) definitely provides a useful tool to analyze possible fixed point structures under automorphisms of a strongly regular graph, we will see in what follows that there are many cases where the more complicated Equality (4) can still be analyzed and provides more interesting information.

We also have the following corollary:

**Corollary 2.2** *Let  $\mathcal{G}$  be a strongly regular graph  $\text{srg}(v, k, \lambda, \mu)$  with integer eigenvalues, and let  $\phi$  be an automorphism of order  $n$  of  $\mathcal{G}$ . Let  $s$  be an integer coprime with  $n$ . Then  $\phi$  and  $\phi^s$  map the same number of vertices to adjacent vertices.*

**Proof.** Because  $s$  is an integer coprime with  $n$  every vertex fixed by  $\phi$  is also fixed by  $\phi^s$ , and vice versa. Hence  $f_\phi = f_{\phi^s}$ . Let  $P$  be the permutation matrix corresponding to the automorphism  $\phi$ . As  $P$  and  $M = A - \nu_3 I$  are both diagonalizable and commute, they can be diagonalized simultaneously (see for example Theorem 1.3.12 in [7]). Hence, for every primitive  $d$ th root of unity  $\xi_d$ , we can find  $a_d^{(\phi)}$  independent vectors  $v_1, \dots, v_{a_d^{(\phi)}}$  that are simultaneously eigenvectors of  $M$  with eigenvalue  $\nu_2 - \nu_3$ , and of  $P$  with eigenvalue  $\xi_d$ . Here the superscript  $(\phi)$  indicates these are the values  $a_d$  corresponding to the automorphism  $\phi$ . Hence  $v_i, i = 1, \dots, a_d^{(\phi)}$ , is an eigenvector of  $P^s M$

with eigenvalue  $\xi_d^s(\nu_2 - \nu_3)$ . As  $s$  is coprime to  $n$  also  $\xi_d^s$  is a primitive  $d$ th root. Hence  $a_d^{(\phi^s)} \geq a_d^{(\phi)}$ . But  $\phi = (\phi^s)^l$  for some  $l$  coprime with  $n$ , and hence  $a_d^{(\phi)} \geq a_d^{(\phi^s)}$ . Thus we conclude that  $a_d^{(\phi)} = a_d^{(\phi^s)}$ . It follows that both  $\phi$  and  $\phi^s$  produce the same left side in Equation (4). Hence also  $g_\phi = g_{\phi^s}$ .  $\square$

In Section 4 we will see that a well-known multiplier result for partial difference sets is a special case of this corollary.

## 2.2 Directed strongly regular graphs

In this short section we note that both Equalities (3), (4) and Congruence (5) have a direct analogue for directed strongly regular graphs. We will not explicitly prove this result, but only point out why one can basically copy the proof of Theorem 2.1 to obtain these analogues.

A directed strongly regular graph with parameters  $(v, k, t, \lambda, \mu)$  is a finite directed graph on  $v$  vertices without loops such that every vertex has in-degree and out-degree equal to  $k$ , each vertex has a constant number  $t$  of undirected edges, there are  $\lambda$  paths of length 2 between  $i$  and  $j$  if there is an edge from  $i$  to  $j$ , and there are  $\mu$  paths of length 2 between  $i$  and  $j$  if there is no edge from  $i$  to  $j$ . Directed strongly regular graphs were introduced by Duval in [5]. The adjacency matrix of a finite directed graph is the square  $(0, 1)$ -matrix  $A$  whose columns and rows are labeled by the vertices and is such that  $A_{ij} = 1$  if and only if there is an edge from vertex  $i$  to vertex  $j$ . The adjacency matrix of a directed strongly regular graph with parameters  $(v, k, t, \lambda, \mu)$  satisfies

$$A^2 + (\mu - \lambda)A - (t - \mu)I = \mu J,$$

$$AJ = JA = kJ.$$

Duval ([5]) showed that the eigenvalues of the adjacency matrix of a directed strongly regular graph that is not an undirected strongly regular graph or a complete graph are always integers, unless  $A$  is a Hadamard matrix. These eigenvalues are

$$\kappa_1 := k,$$

$$\kappa_2 := \frac{1}{2}(\lambda - \mu + \sqrt{D}),$$

$$\kappa_3 := \frac{1}{2}(\lambda - \mu - \sqrt{D}),$$

with respective multiplicities

$$m_1 := 1,$$

$$m_2 := \frac{1}{2} \left( v - 1 - \frac{2k + (v - 1)(\lambda - \mu)}{\sqrt{D}} \right)$$

and

$$m_3 := \frac{1}{2} \left( v - 1 + \frac{2k + (v - 1)(\lambda - \mu)}{\sqrt{D}} \right),$$

where  $D = (\lambda - \mu)^2 + 4(t - \mu)$ .

Let  $A$  be the adjacency matrix of a directed strongly regular graph, and let  $P$  be the permutation matrix of an automorphism of order  $n$  of this graph. As before  $PAP^T = A$ , and  $P^{-1} = P^T$ , so that  $A$  and  $P$  commute. This implies that the eigenvalues of  $PM$  are the eigenvalues of  $M = A - rI$  multiplied by  $n$ th roots of unity. Also, if the eigenvalues of  $A$  are integers, we are guaranteed that the multiplicity of the eigenvalue  $\xi_d \rho$  of  $PM$ , where  $\xi_d$  is a  $d$ th root of unity and  $\rho$  is an eigenvalue of  $M$ , will not depend on specific  $d$ th root of unity. One now easily obtains the following result:

**Theorem 2.3** *Let  $\mathcal{G}$  be a directed strongly regular graph that is not undirected, not a complete graph, and whose adjacency matrix is not a Hadamard matrix. Let  $\phi$  be an automorphism of order  $n$  of  $\mathcal{G}$ . Let  $\mu(\cdot)$  be the Möbius function. Then for every integer  $r$  and all positive divisors  $d$  of  $n$ , there are non-negative integers  $a_d$  and  $b_d$  such that*

$$k - r + \sum_{d|n} a_d \mu(d)(\kappa_2 - r) + \sum_{d|n} b_d \mu(d)(\kappa_3 - r) = -rf + g, \quad (6)$$

where  $f$  is the number of fixed vertices of  $\phi$  and  $g$  the number of vertices that are adjacent to their image under  $\phi$ . As a consequence the following equation and congruence hold:

$$k - \kappa_3 + \sum_{d|n} a_d \mu(d)(\kappa_2 - \kappa_3) = -\kappa_3 f + g \quad (7)$$

and

$$k - \kappa_3 \equiv -\kappa_3 f + g \pmod{\kappa_2 - \kappa_3}. \quad (8)$$

Unfortunately there is no nice analogue of Corollary 2.2, as one can not guarantee that the adjacency matrix of a directed strongly regular graph is diagonalizable. However, if one knows that  $A$  is diagonalizable the result of Corollary 2.2 remains valid for directed strongly regular graphs.

### 3 Automorphisms of prime order

In this section we provide the basic idea on how to analyze Equations (4) and (7). The two examples in Section 5 will further develop this idea.

As before let  $\mathcal{G}$  be a strongly regular graph  $\text{srg}(v, k, \lambda, \mu)$  with integer eigenvalues. Assume  $\phi$  is an automorphism of order  $p$ , prime, of  $\mathcal{G}$ . Then we can use the result of theorem 2.1 to obtain an interesting divisibility condition. Setting  $r = \nu_3$  we obtain  $k - \nu_3 + \sum_{d|p} a_d \mu(d)(\nu_2 - \nu_3) = -\nu_3 f + g$ . As  $p$  is prime we have  $\mu(1) = 1$  and  $\mu(p) = -1$ . Also  $a_1 + (p-1)a_p = m_2$ . We obtain the following system of linear equations in  $a_1$  and  $a_p$ :

$$\begin{cases} a_1(\nu_2 - \nu_3) - a_p(\nu_2 - \nu_3) &= -\nu_3(f - 1) + g - k \\ a_1 + (p-1)a_p &= m_2. \end{cases}$$

This system can easily be solved for  $a_1$  and  $a_p$  which should be non-negative integers. This can be of particular interest if one is trying to disprove the existence of a hypothetical strongly regular graph which should admit certain automorphisms, for example a certain Cayley graph (see Sections 4 and 5). In what follows we will see how in certain cases it is possible to obtain results that go beyond automorphisms of prime order.

A similar result can be obtained for directed strongly regular graphs in the obvious way.

### 4 Partial difference sets in abelian groups

We will now focus on strongly regular graphs where the existence of a certain automorphism is a priori known. Strongly regular Cayley graphs on abelian groups are important graphs in this category. In this case the graph is equivalent to a so-called partial difference set (PDS). We will recover some known results on these objects with new elementary proofs, as well as some new results. We first review some basic definitions.

Let  $G$  be a finite abelian group of order  $v$ , and let  $\mathcal{D}$  be a  $(v, k, \lambda, \mu)$  partial difference set in  $G$ , that is,  $\mathcal{D}$  is a  $k$ -subset of  $G$  with the property that the expressions  $\phi\psi^{-1}$ ,  $\phi, \psi \in \mathcal{D}$ , represent each nonidentity



element in  $\mathcal{D}$  exactly  $\lambda$  times, and each nonidentity element of  $G$  not in  $\mathcal{D}$  exactly  $\mu$  times. Further assume that  $\mathcal{D}^{(-1)} = \mathcal{D}$  (that is, if  $\phi \in \mathcal{D}$ , then so is  $\phi^{-1}$ ) and  $e \notin \mathcal{D}$ , where  $e$  is the identity in  $G$ , that is,  $\mathcal{D}$  is a so-called regular partial difference set. Then it is well known (see e.g. [9]) that the Cayley graph  $\mathcal{G} := (G, \mathcal{D})$  is a strongly regular graph with parameters  $\text{srg}(v, k, \lambda, \mu)$ . Recall that two elements  $\phi$  and  $\psi$  of  $G$  are adjacent in  $\mathcal{G}$  if and only if  $\psi\phi^{-1} \in \mathcal{D}$ . Also, if  $\lambda \neq \mu$  then  $\mathcal{D}^{(-1)} = \mathcal{D}$  is automatically fulfilled (see [9]).

Let  $\mathcal{G} = (G, \mathcal{D})$  be a strongly regular Cayley graph on an abelian group  $G$ , and assume that  $\mathcal{G}$  is not a conference graph. Then the nonidentity elements of  $G$  act in an obvious way as fixed point free automorphisms on  $\mathcal{G}$ . Furthermore, such automorphism,  $\phi$ , maps either every vertex to an adjacent vertex (if and only if  $\phi \in \mathcal{D}$ ), or maps no vertex to an adjacent vertex. The latter can be seen as follows. Assume  $\phi$  maps vertex  $\psi$  to adjacent vertex  $\psi\phi$ . Then clearly  $(\psi\phi)\psi^{-1} = \phi \in \mathcal{D}$ . For every other vertex  $\gamma$  we then have that  $(\gamma\phi)\gamma^{-1} = \phi \in \mathcal{D}$ , and hence every vertex is mapped to an adjacent vertex. We obtain the following result:

**Corollary 4.1** *With the above notation, it holds that*

$$2k - \lambda + \mu \equiv 0 \equiv v \pmod{\sqrt{\Delta}}.$$

**Proof.** First let  $\phi$  be an element of  $G \setminus (\mathcal{D} \cup \{e\})$ . Then we can apply Congruence 5 with  $f = 0$  and  $g = 0$ . We obtain

$$k - \frac{1}{2}(\lambda - \mu - \sqrt{\Delta}) \equiv 0 \pmod{\sqrt{\Delta}}. \quad (9)$$

Next, let  $\phi$  be an element of  $\mathcal{D}$ . Then we can apply Congruence 5 with  $f = 0$  and  $g = v$ . We obtain

$$k - \frac{1}{2}(\lambda - \mu - \sqrt{\Delta}) \equiv v \pmod{\sqrt{\Delta}}.$$

Combining both Congruences proves the result.  $\square$

This congruence was obtained with a different proof by S.L. Ma [9].

Corollary 2.2 can be used to obtain a multiplier result that was previously obtained by Ma [9].

**Corollary 4.2** *Let  $\mathcal{D}$  be a regular  $(v, k, \lambda, \mu)$  partial difference set not containing the identity in the abelian group  $G$ . Furthermore assume  $\Delta$  is a perfect square. Then  $\mathcal{D}^{(s)} = \mathcal{D}$  for every  $s$  coprime to  $v$ .*

**Proof.** This follows immediately from Corollary 2.2 and the fact that an element of  $G$  belongs to  $\mathcal{D}$  if and only if it maps every vertex to an adjacent vertex in the corresponding Cayley graph.  $\square$

We next look at Equality (4). It is obvious that one obtains two equalities, one for  $\phi \notin \mathcal{D}$ , and one for  $\phi \in \mathcal{D}$ .

If we assume that  $\phi$  has prime order the results from Section 3 can be applied, and we obtain:

If  $\phi \notin \mathcal{D}$  then  $a_p = \frac{-v(\lambda-\mu-\sqrt{\Delta})}{2p\sqrt{\Delta}}$  must be an integer. If  $\phi \in \mathcal{D}$  then  $a_p = \frac{-2v-v(\lambda-\mu-\sqrt{\Delta})}{2p\sqrt{\Delta}}$  must be an integer. At first sight this does not seem to provide much information (because  $p$  definitely divides  $v$ ), however, if we use this as the basis for studying automorphism of higher order useful conclusions can be drawn (see Section 5).

## 5 Two examples

We will illustrate how the ideas developed in this paper can be used by disproving the existence of a  $(100, 33, 8, 12)$  and a  $(100, 36, 14, 12)$  regular partial difference set in an Abelian group of order 100. These were the only two parameter sets for regular PDS in Abelian groups of size at most 100 for which (non)-existence had not been settled (see [10], [11]). It is worthwhile to note that a  $(100, 36, 14, 12)$  PDS does exist in non-Abelian groups of order 100 (see [8]). We start with the  $(100, 33, 8, 12)$  case.

Assume by way of contradiction that  $\mathcal{D}$  is a  $(100, 33, 8, 12)$  regular PDS in the Abelian group  $G$ . We first show that  $G$  cannot contain a subgroup of order 25 by analyzing elements of order  $5^k$ .

ELEMENTS OF ORDER 5. Let  $\phi$  be an element of order 5 in  $G$ . We compute  $a_1^{(\phi)}$  and  $a_5^{(\phi)}$ .

$o(\phi) = 5$	$a_1^{(\phi)}$	$a_5^{(\phi)}$
$\phi \in \mathcal{D}$	18	12
$\phi \notin \mathcal{D}$	10	14

ELEMENTS OF ORDER 25. Next assume  $\phi$  is an element of order 25 in  $G$ . Then  $\phi^5$  is an element of order 5, and we obtain (using the same ideas as in the proof of Corollary 2.2):

$$a_1^{(\phi^5)} = a_1^{(\phi)} + 4a_5^{(\phi)}, \quad \text{and} \quad 4a_5^{(\phi^5)} = 20a_{25}^{(\phi)}.$$

From the last equation we see that  $a_5^{(\phi^5)}$  must be a multiple of 5, however, a quick inspection of the table with multiplicities for elements of order 5 shows this is never the case. Hence  $G$  does not contain elements of order 25, and  $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$  or  $G \cong \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5$ .

By Corollary 2.2 the elements of order 5, 10, and 20 in  $\mathcal{D}$  come in sets of 4, 4 and 8 respectively. Elements of order 4 in  $\mathcal{D}$  come in sets of two. As the size of  $\mathcal{D}$  is 33 it now easily follows that  $\mathcal{D}$  contains a unique element of order 2, while all other elements in  $\mathcal{D}$  have order divisible by 5. We now look at the elements of  $G$  whose order is divisible by 2.

ELEMENTS OF ORDER 2 If  $\phi$  is an element of order 2 in  $G$  then we obtain the following multiplicities:

$o(\phi) = 2$	$a_1^{(\phi)}$	$a_2^{(\phi)}$
$\phi \in \mathcal{D}$	36	30
$\phi \notin \mathcal{D}$	31	35

ELEMENTS OF ORDER 10 Now let  $\phi$  be an element in  $G$  of order 10. Using that  $\phi^5$  has order 2 and  $\phi^2$  order 5 we obtain

$$a_1^{(\phi^5)} = a_1^{(\phi)} + 4a_5^{(\phi)}, \quad \text{and} \quad a_2^{(\phi^5)} = a_2^{(\phi)} + 4a_{10}^{(\phi)},$$

$$a_1^{(\phi^2)} = a_1^{(\phi)} + a_2^{(\phi)}, \quad \text{and} \quad 4a_5^{(\phi^2)} = 4a_5^{(\phi)} + 4a_{10}^{(\phi)},$$

and finally from Equation (4)

$$40 + (a_1^{(\phi)} - a_2^{(\phi)} - a_5^{(\phi)} + a_{10}^{(\phi)})10 = g,$$

where  $g = 0$  or  $g = 100$  depending on whether  $\phi \notin \mathcal{D}$  or  $\phi \in \mathcal{D}$ . There are eight cases to consider depending on whether  $\phi, \phi^2, \phi^5$  all or not belong to  $\mathcal{D}$ .

We obtain

$o(\phi) = 10$	$a_1^{(\phi)}$	$a_2^{(\phi)}$	$a_5^{(\phi)}$	$a_{10}^{(\phi)}$
$\phi^5 \in \mathcal{D}, \phi^2 \in \mathcal{D}, \phi \in \mathcal{D}$	12	6	6	6
$\phi^5 \in \mathcal{D}, \phi^2 \in \mathcal{D}, \phi \notin \mathcal{D}$	8	10	7	5
$\phi^5 \in \mathcal{D}, \phi^2 \notin \mathcal{D}, \phi \in \mathcal{D}$	8	2	7	7
$\phi^5 \in \mathcal{D}, \phi^2 \notin \mathcal{D}, \phi \notin \mathcal{D}$	4	6	8	6
$\phi^5 \notin \mathcal{D}, \phi^2 \in \mathcal{D}, \phi \in \mathcal{D}$	11	7	5	7
$\phi^5 \notin \mathcal{D}, \phi^2 \in \mathcal{D}, \phi \notin \mathcal{D}$	7	11	6	6
$\phi^5 \notin \mathcal{D}, \phi^2 \notin \mathcal{D}, \phi \in \mathcal{D}$	7	3	6	8
$\phi^5 \notin \mathcal{D}, \phi^2 \notin \mathcal{D}, \phi \notin \mathcal{D}$	3	7	7	7

First note that from this table we see that possibilities 1, 5 and 6 cannot occur. The reason for this is that  $\phi$  acts with 10 orbits of length 10, and hence has each 10th root of unity as an eigenvalue with multiplicity exactly 10. This implies that none of the  $a_i^{(\phi)}$ ,  $i = 1, 2, 5, 10$ , can be larger than 10.

We now exclude  $G \cong \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5$  and  $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$  one by one. First assume  $G \cong \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5$ . Then  $G$  would contain an element  $\phi$  of order 20, yielding

$$4a_{10}^{(\phi^2)} = 8a_{20}^{(\phi)}, \quad \text{and} \quad a_2^{(\phi^2)} = 2a_4^{(\phi)}.$$

As every element of order 10 is the square of an element of order 20 this further excludes, by the obvious parity argument, possibilities 2, 3, 7 and 8 from the above table. Hence only possibility 4 is left. As every element of order 5 is the square of an element of order 10, it follows that  $\mathcal{D}$  does not contain any element of order 5 or 10, and hence  $\mathcal{D}$  consists of the unique element of order 2 and 32 elements of order 20. However, it is easy to check that the elements of order 4 can never be written as a difference of two elements of order 20 or as the difference of an element of order 20 and the unique element of order 2. This contradicts  $\mathcal{D}$  is a partial difference set with the given parameters.

Finally assume that  $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$ . We already know that  $\mathcal{D}$  must contain a unique element of order 2, say  $\iota$ . Now assume that  $\gamma$  would be an element of order 5 in  $\mathcal{D}$ , and let  $\kappa$  be an element of order 2 not in  $\mathcal{D}$ . Let  $\gamma'$  be the unique element such that  $\gamma'^2 = \gamma$ . Then  $\phi = \kappa\gamma'$  has order 10 and  $\phi^2 = \gamma \in \mathcal{D}$ , whereas  $\phi^5 = \kappa \notin \mathcal{D}$ . Hence we must be in case 5 or 6 of our table. However, these cases were previously excluded. This implies that  $\mathcal{D}$  cannot contain any element of order 5. For convenience let us write the elements of  $G$  as  $(a, b, c, d)$ , where addition is done component wise modulo 2 in the first two components and modulo 5 in the two last components. Without loss of generality we can assume that  $\iota = (1, 1, 0, 0)$ . All other elements of  $\mathcal{D}$  are of the form  $(1, 0, a, b)$ ,  $(1, 1, a, b)$  or  $(0, 1, a, b)$ , where  $(a, b) \neq (0, 0)$ . It is easy to see that the only way to write  $(1, 0, 0, 0)$  as a difference of elements in  $\mathcal{D}$  is as  $(1, 0, 0, 0) = (1, 1, a, b) - (0, 1, a, b) = (0, 1, a, b) - (1, 1, a, b)$ . However, as the elements of order 10 in  $\mathcal{D}$  come in groups of 4, this implies that the differences in  $\mathcal{D}$  that produce  $(1, 0, 0, 0)$  come in sets of 8. But the  $\mu$ -parameter for this partial difference set equals 12, not a multiple of 8, the final contradiction.

Next we exclude the existence of a  $(100, 36, 14, 12)$  regular PDS in an Abelian group  $G$ . As the ideas and techniques are very similar we will be briefer in our arguments.

ELEMENTS OF ORDER 5.

$o(\phi) = 5$	$a_1^{(\phi)}$	$a_5^{(\phi)}$
$\phi \in \mathcal{D}$	12	6
$\phi \notin \mathcal{D}$	4	8

Because  $a_5^{(\phi)}$  is never divisible by 5 this again excludes the existence of a subgroup of order 25 in  $G$ .

It is useful to make an argument based on Corollary 2.2 at this point. As there are only 3 elements in  $G$  whose order is a power of 2, the elements of order divisible by 5 in  $\mathcal{D}$  come in sets whose size is a multiple of 4, and  $|\mathcal{D}|$  is divisible by 4, it follows that  $\mathcal{D}$  does not contain any element of order a power of 2. This allows us to only compute partial tables of multiplicities.

ELEMENTS OF ORDER 2, 4 AND 10.

$o(\phi) = 2$	$a_1^{(\phi)}$	$a_2^{(\phi)}$
$\phi \notin \mathcal{D}$	16	20

$o(\phi) = 4$	$a_1^{(\phi)}$	$a_2^{(\phi)}$	$a_4^{(\phi)}$
$\phi \notin \mathcal{D}$	6	10	10

$o(\phi) = 10$	$a_1^{(\phi)}$	$a_2^{(\phi)}$	$a_5^{(\phi)}$	$a_{10}^{(\phi)}$
$\phi^5 \notin \mathcal{D}, \phi^2 \in \mathcal{D}, \phi \in \mathcal{D}$	8	4	2	4
$\phi^5 \notin \mathcal{D}, \phi^2 \in \mathcal{D}, \phi \notin \mathcal{D}$	4	8	3	3
$\phi^5 \notin \mathcal{D}, \phi^2 \notin \mathcal{D}, \phi \in \mathcal{D}$	4	0	3	5
$\phi^5 \notin \mathcal{D}, \phi^2 \notin \mathcal{D}, \phi \notin \mathcal{D}$	0	4	4	4

Now first assume  $G \cong \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5$ , and let  $\phi$  be an element of order 20. Then, as before, we see that  $a_2^{(\phi^2)}$  and  $a_{10}^{(\phi^2)}$  must be even. Hence only case 1 ( $\phi^2 \in \mathcal{D}$ ) and case 4 ( $\phi^2 \notin \mathcal{D}$ ) in the previous table can occur. We obtain

$o(\phi) = 20$	$a_1^{(\phi)}$	$a_2^{(\phi)}$	$a_4^{(\phi)}$	$a_5^{(\phi)}$	$a_{10}^{(\phi)}$	$a_{20}^{(\phi)}$
$\phi^2 \in \mathcal{D}, \phi \in \mathcal{D}$	6	2	2	0	2	2
$\phi^2 \in \mathcal{D}, \phi \notin \mathcal{D}$	2	6	2	1	1	2
$\phi^2 \notin \mathcal{D}, \phi \in \mathcal{D}$	2	-2	2	1	3	2
$\phi^2 \notin \mathcal{D}, \phi \notin \mathcal{D}$	-2	2	2	2	2	2

As  $\phi$  acts with 20 orbits of length 5, it has each 20th root of unity as an eigenvalue with multiplicity exactly 5. This implies that none of the  $a_i^{(\phi)}$ ,  $i = 1, 2, 4, 5, 10, 20$ , can be larger than 5. This excludes the first two possibilities. Finally the last two possibilities are excluded as multiplicities have to be non-negative integers.

Finally assume that  $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$ . Let  $\iota$  be any element of order 2. If  $\iota = \alpha\beta^{-1}$ , for  $\alpha, \beta \in \mathcal{D}$ , then also  $\iota = \beta\alpha^{-1}$ . As the elements of  $\mathcal{D}$  have order 5 or 10 they come in sets of 4. Hence the number of ways in which  $\iota$  can be written as a difference of elements of  $\mathcal{D}$  is a multiple of 8. However,  $\mu = 12$ , the final contradiction.

## 6 Projective two-weight sets

In this last section we will shortly describe how the results of this paper can be used in the analysis of hypothetical projective two-weight set with given parameters.

Let  $\text{PG}(n, q)$  be the  $n$ -dimensional projective space over the field  $\mathbb{F}_q$ . A projective two-weight set  $K$  of type  $(w_1, w_2)$ ,  $w_1 \neq w_2 \neq 0$ , in  $\text{PG}(n, q)$  is a set of points in  $\text{PG}(n, q)$  with the property that every hyperplane of  $\text{PG}(n, q)$  intersects  $K$  in either  $w_1$  or  $w_2$  points. It is well known that such sets are equivalent to linear two-weight codes and give rise to strongly regular graphs (see for example [2]). Here we will only describe how these sets give rise to a strongly regular graph, and then apply the results earlier obtained in the paper.

From here on, let  $K$  be a two-weight set of type  $(w_1, w_2)$  and size  $N$  in  $\text{PG}(n, q)$ . Embed  $\text{PG}(n, q)$  as a hyperplane in  $\text{PG}(n + 1, q)$ . Construct the graph  $\mathcal{G}$  as follows: the vertices of  $\mathcal{G}$  are the points of  $\text{PG}(n + 1, q) \setminus \text{PG}(n, q)$ ; two vertices  $g$  and  $h$  of  $\mathcal{G}$  are adjacent if and only if the projective line  $\langle g, h \rangle$  intersects  $\text{PG}(n, q)$  in a point of  $K$ . Then it is well known that  $\mathcal{G}$  is strongly regular with parameters  $v = q^{n+1}$ ,  $k = (q - 1)N$ ,  $\lambda = k^2 + 3k - (k + 1)q(2n - w_1 - w_2)$ ,  $\mu = (n - w_1)(n - w_2)/q^{n-1}$  (see [2]). It is obvious that the group  $T$  of translations of  $\text{PG}(n + 1, q)$  with axis  $\text{PG}(n, q)$  acts as a sharply transitive abelian group of automorphisms. Now fix any point (vertex of  $\mathcal{G}$ )  $g$  of  $\text{PG}(n + 1, q) \setminus \text{PG}(n, q)$ , and identify any point  $h$  of  $\text{PG}(n + 1, q) \setminus \text{PG}(n, q)$  with the unique element  $\tau$  of  $T$  with the property that  $g^\tau = h$ . If under this correspondence  $\mathcal{D}$  is the subset of  $T$  corresponding to the vertices of  $\mathcal{G}$  adjacent to  $p$ , then it is clear that  $\mathcal{D}$  is a regular PDS in  $T$ , and that  $\mathcal{G} = (T, \mathcal{D})$ . Hence all results from

Section 4 can be applied. However, the graph  $\mathcal{G}$  admits another interesting group of automorphisms. Again, let  $g$  be a fixed chosen point of  $\text{PG}(n+1, q) \setminus \text{PG}(n, q)$ . Then the group  $H$  of homologies with center  $g$  and axis  $\text{PG}(n, q)$  will act obviously as a group of automorphisms of  $\mathcal{G}$ . Any non-identity element of  $H$  will have exactly one fixed vertex ( $g$ ) and map  $k = (q-1)N$  vertices to adjacent vertices. First note that simply applying Congruence (5) does not produce any useful results (it simply yields  $k - \nu_3 \equiv k - \nu_3 \pmod{\nu_2 - \nu_3}$ ). However, just as was discussed in Sections 4 and 5, analyzing Equation (4) does provide new information. The group  $H$  has order  $q-1$ , and for every prime divisor  $p$  of  $q-1$  we can pick an element  $\phi$  of  $H$  of that order and apply the result of Section 3. We obtain that  $a_1^{(\phi)} = a_p^{(\phi)}$  and  $a_1^{(\phi)} = m_2/p$ . As  $p$  divides  $v-1 = q^{n+1}-1$  this typically is not a strong condition. However, it might, just as in Section 5, be used as the basis to analyze automorphisms of higher order in  $H$ .

## Acknowledgement

The authors want to thank Tim Penttila for suggesting to look at directed strongly regular graphs.

## References

- [1] C.T. Benson, On the structure of generalized quadrangles, *J. Algebra* **15**, 443-454, 1970.
- [2] R. Calderbank and W.M. Kantor, The geometry of two-weight codes, *Bull. London Math. Soc.* **18**, 97-122, 1986.
- [3] S. De Winter, Partial geometries  $\text{pg}(s, t, 2)$  with an abelian Singer group and a characterization of the van Lint-Schrijver partial geometry, *J. Algebraic Combin.* **24**, 285-297, 2006.
- [4] S. De Winter and K. Thas, The automorphism group of Payne derived generalized quadrangles, *Advances in Mathematics* **214**, 146-156, 2007.
- [5] A. Duval, A directed graph version of strongly regular graphs, *J. Combin. Theory Series A*, **47**, 71-100, 1988.
- [6] C. Godsil and G. Royle, *Algebraic Graph Theory*, Springer-Verlag, 2004.

- [7] R.A. Horn and C.R. Johnson, *Matrix Analysis, 2nd Ed.*, Cambridge University Press, 2013.
- [8] L.K. Jørgensen and M. Klin, Switching of edges in strongly regular graphs. I. A family of partial difference sets on 100 vertices, *Electron. J. Combin.* **10** (1), 2003.
- [9] S.L. Ma, A survey of partial difference sets, *Designs, Codes, Cryptogr.* **4**, 221-261, 1994.
- [10] S.L. Ma, Some necessary conditions on the parameters of partial difference sets, *J. Statist. Plann. Inference* **62**, 47-56, 1997.
- [11] M. H. Nam, *A table of partial difference sets in abelian groups*, UROPS report (supervised by S. L. Ma), National University of Singapore, 2003/2004.
- [12] S.E. Payne and J.A. Thas, *Finite generalized quadrangles*, Pitman, Boston- London-Melbourne, 1984
- [13] B. Temmermans, J.A. Thas and H. Van Maldeghem, On collineations and dualities of finite generalized polygons, *Combinatorica* **29**, 569-594, 2009.